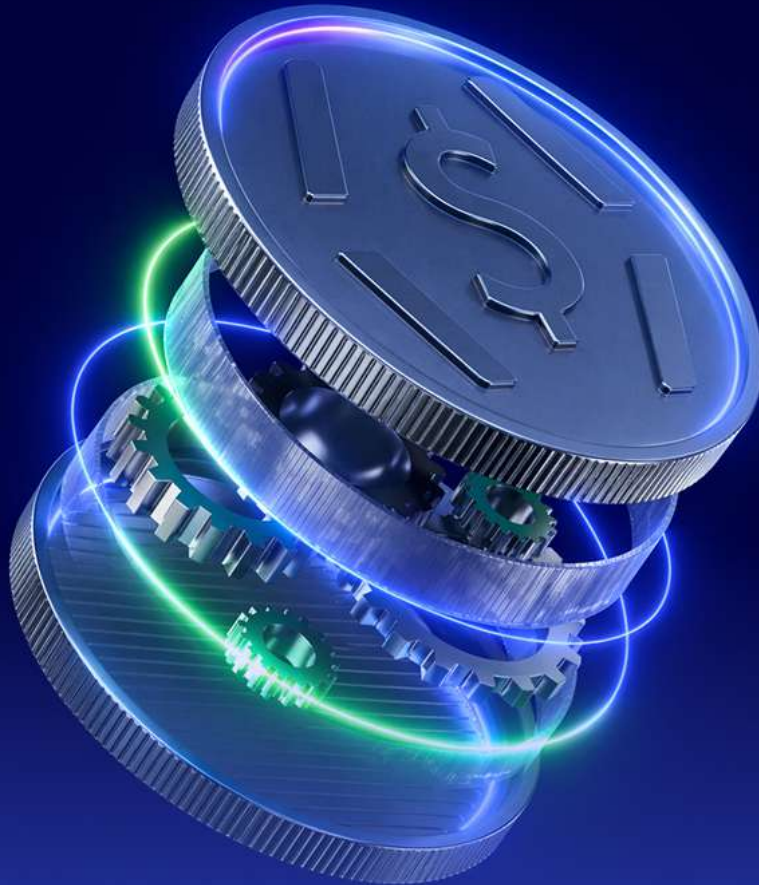


Wenia

USDW

Whitepaper



Wenia USDW - Whitepaper

USDW es un activo digital estable (stablecoin) creado por Wenia, referenciado 1:1 con el dólar de los Estados Unidos y diseñado para conectar a América Latina con la nueva economía digital.

Palabras clave: token respaldado con activos, seguridad blockchain, finanzas descentralizadas, regulación de activos digitales, tokens ERC20, computación multipartita, auditorías de contratos inteligentes, cumplimiento para stablecoins, transparencia.

1. Introducción

En los últimos años, los activos digitales han experimentado un crecimiento significativo en su adopción por parte de personas y entidades. Su desarrollo ha sido impulsado por la tecnología de registro distribuido o blockchain, que permite transferir y almacenar activos de manera segura, transparente y eficiente. Además, cualquier interesado puede verificar las transacciones en cadena, lo que aporta trazabilidad y capacidad de auditoría.

Los activos digitales también pueden programarse mediante contratos inteligentes. Esta capacidad permite automatizar casos de uso como pagos entre participantes, liquidación de acuerdos financieros y otros procesos comerciales. En consecuencia, las transacciones pueden ser más rápidas, seguras y eficientes, reduciendo fricciones operativas.

Sin embargo, la volatilidad de precio de muchos activos digitales ha limitado su

adopción como unidad de cuenta y medio de intercambio. En respuesta, la industria ha desarrollado las stablecoins.

Las stablecoins son tokens criptográficos emitidos en una blockchain y generalmente referenciados a una moneda fiat. Su objetivo es mantener un valor estable, normalmente en una proporción 1:1 con la moneda de referencia. Para lograrlo, el emisor constituye previamente una reserva de activos altamente líquidos y de baja volatilidad. Estas reservas se mantienen separadas de las cuentas operativas del emisor y pueden ser auditadas de forma independiente para respaldar la transparencia y la seguridad.

Wenia Ltd. presenta USDW, su stablecoin denominada en dólares de los Estados Unidos. Wenia Ltd. está regulada por la Autoridad Monetaria de Bermudas y cuenta con una licencia Clase F que autoriza, entre otras actividades, la emisión, venta y redención de activos digitales. USDW está diseñado como un token confiable y seguro, respaldado por activos altamente líquidos y de bajo riesgo, como efectivo e instrumentos de renta fija de alta calidad crediticia, con el objetivo de mantener una referencia estricta 1:1 con el dólar estadounidense.

1.1 Visión

La visión de USDW es apoyar el desarrollo de la economía digital en América Latina conectando el dinero de los usuarios con la industria de activos digitales. USDW facilita el intercambio con otros criptoactivos y puede utilizarse para cumplir obligaciones entre usuarios de Wenia que lo acepten.

Con el tiempo, se espera que USDW pueda almacenarse y transferirse en plataformas y billeteras adicionales fuera del ecosistema

Wenia. Esta expansión podría permitir a desarrolladores crear aplicaciones descentralizadas que utilicen el dólar estadounidense como unidad de cuenta, promoviendo innovación y soluciones financieras más accesibles.

Al aprovechar herramientas Web3 como los exploradores de bloques, USDW también funciona como un mecanismo de auditoría en tiempo real de las reservas que respaldan su emisión, reforzando la transparencia y la confianza.

1.2 Propuesta de valor

USDW combina la estabilidad de una referencia al dólar estadounidense con la eficiencia, transparencia y capacidad de programación de la tecnología blockchain.

Además, opera dentro de los estándares establecidos por la Digital Asset Business Act 2018 de Bermudas y la normativa aplicable a negocios de activos digitales y stablecoins de moneda única. Este marco regula todo el ciclo de vida del activo, desde su emisión y custodia hasta su transferencia, aportando una capa adicional de supervisión y confianza.

Las siguientes secciones describen la implementación técnica de USDW, su modelo de reservas, su arquitectura de seguridad y su contexto regulatorio.

2. Tecnología

USDW está construido sobre el estándar ERC20, lo que permite desplegar contratos inteligentes seguros y eficientes, ampliamente compatibles con billeteras,

proveedores de infraestructura y otras aplicaciones blockchain.

Además de aprovechar librerías de código abierto, Wenia desarrolló un estándar mejorado llamado TokenizationW para incorporar mejores prácticas de la industria y funcionalidades avanzadas de cumplimiento. Este estándar fue auditado externamente por OpenZeppelin desde su primera versión. USDW fue desplegado en la red principal de Ethereum utilizando este estándar actualizado.

TokenizationW incorpora lógica de prueba de reservas que restringe la emisión de tokens con base en información externa de la reserva y controles sobre la vigencia de los datos. También incluye funciones de cumplimiento como listas de restricciones y listas de autorizaciones, la posibilidad de eliminar fondos de direcciones restringidas en circunstancias excepcionales, referencias legales en cadena mediante funciones vinculadas a documentos, y mejoras de eficiencia en el uso de gas.

Los protocolos de seguridad y las políticas de ejecución del contrato inteligente de USDW están diseñados para asegurar confiabilidad, integridad y transparencia durante todo su ciclo de vida.

3. USDW

USDW está diseñado para mantener un precio de referencia 1:1 con el dólar de los Estados Unidos mediante una reserva de activos líquidos financiada con recursos del balance propio de Wenia.

3.1 Fundamento

La reserva está compuesta principalmente por efectivo y activos denominados en dólares con alta calidad crediticia, incluidos depósitos, bonos del Tesoro de los Estados Unidos, fondos de mercado monetario y otros instrumentos de renta fija altamente calificados.

Estas reservas son administradas por Banco Agrícola en El Salvador y se mantienen separadas de las cuentas operativas de Wenia, con el fin de respaldar la existencia y liquidez de los activos y facilitar su revisión independiente.

USDW está disponible para su conversión en criptoactivos soportados por Wenia, manteniendo su referencia 1:1 con el dólar estadounidense.

3.2 Ciclo de vida

Las reservas que respaldan USDW se administran mediante una estructura fiduciaria segregada mantenida con una entidad supervisada por una autoridad regulatoria.

Antes de emitir USDW, se verifica la suficiencia de los activos de reserva. El valor de mercado de estos activos limita el monto total que puede emitirse, manteniendo una relación mínima de respaldo 1:1.

La fiducia también mantiene una reserva adicional de liquidez destinada a cubrir gastos operativos y mitigar riesgos de mercado. Las inversiones se limitan a instrumentos de alta liquidez y corta duración. Se realizan auditorías periódicas y

los cambios relevantes en la estrategia de reserva están sujetos a gobierno interno y reporte regulatorio.

3.2.1 Gestión del suministro circulante

USDW se emite por lotes mediante un proceso programado, ajustando la oferta según la demanda en intervalos predefinidos. Esto optimiza los costos de emisión y facilita la coordinación con la estructura de reservas.

La emisión no ocurre por cada transacción individual, sino de forma anticipada y siempre respaldada por activos disponibles en reserva.

Cuando un titular desea redimir USDW, Wenia recompra el activo digital. En periodos de baja demanda, puede reducir el suministro mediante la quema de tokens.

3.2.1.1 Descripción general de riesgos asociados con USDW

a) Riesgo de despegue: posibilidad de que USDW pierda su referencia 1:1 con el dólar estadounidense. Wenia mitiga este riesgo mediante monitoreo continuo de la reserva y un plan de fondeo de contingencia.

b) Riesgo de liquidez: riesgo de no poder atender obligaciones a tiempo por insuficiencia de activos líquidos. Wenia prioriza la gestión de liquidez y utiliza modelos VaR y pruebas de estrés.

c) Metodología VaR: durante los primeros 90 días de operación, casi el 100% de las

reservas se mantuvo en efectivo para evaluar necesidades de liquidez.

Posteriormente se aplica una metodología de simulación histórica con una ventana de 90 días, un horizonte de 1 día y un nivel de confianza del 99,99%.

d) Pruebas de estrés: Wenia realiza escenarios de estrés considerando cambios en tasas de interés, volúmenes de negociación, noticias de mercado y comportamiento de redención de clientes.

e) Riesgo operativo: incluye fallas de sistemas, error humano y ciberataques. Wenia mantiene políticas y procedimientos de resiliencia, controles duales, segregación de funciones y monitoreo de acciones críticas del contrato inteligente.

f) Riesgo de mercado: movimientos adversos del mercado pueden afectar el valor de los activos de reserva. Estos riesgos se monitorean mediante modelos de simulación y pruebas de estrés.

3.2.1.2 Políticas y procedimientos

a) Gestión centralizada de liquidez: Wenia gestiona la liquidez de manera centralizada, considerando perfiles de liquidez actuales y potenciales a nivel de grupo.

b) Reserva de liquidez: Wenia mantiene una reserva compuesta por efectivo y títulos de alta calidad emitidos por gobiernos o entidades privadas con fuerte calidad

crediticia, con duración máxima de 12 meses.

c) Plan de fondeo de contingencia (CFP): en escenarios de estrés, el CFP identifica fuentes alternativas de liquidez y establece procedimientos para gestionar la liquidez de manera efectiva, incluyendo caja operativa, líneas de crédito revolvente, liquidación de activos y endeudamiento colateralizado.

d) Supervisión y monitoreo: se realizan pruebas de estrés mensuales y seguimiento diario de liquidez y fondeo, con reporte a la alta dirección y a la junta directiva.

3.2.2 Transparencia

La transparencia es esencial para la confianza en cualquier sistema financiero, especialmente en el ecosistema de stablecoins. Wenia la respalda mediante atestaciones externas y el uso de infraestructura de oráculos blockchain.

Bajo el marco regulatorio de Bermudas para activos digitales, Wenia mantiene un compromiso con la transparencia y la gestión prudente de riesgos. Esto incluye prueba de reservas, arreglos de custodia seguros y segregación de activos relevantes conforme a los requisitos aplicables.

A la fecha de publicación de este borrador, Arévalo Segovia y Asociados, S.A. de C.V. realiza atestaciones periódicas de las reservas de Wenia para verificar que los activos en reserva sean suficientes para respaldar el USDW en circulación.

Para reforzar la transparencia y la seguridad, el contrato inteligente de USDW está diseñado para interactuar con la red de oráculos de Chainlink. Esta integración permite recibir datos externos sobre el estado de la reserva antes de nuevas emisiones.

Dirección del oráculo de Chainlink:
<https://etherscan.io/address/0xe2c4e28d938aa42a5c5edd5193f7bd2a972bf7bf>

Dirección del proxy del token USDW:
<https://etherscan.io/token/0x131522cad80c0c45c014eb484af41df5af311721>

El contrato inteligente de USDW incorpora mecanismos automáticos que restringen el mintage de nuevos tokens cuando la reserva verificada no es suficiente. Si la cantidad a emitir, sumada al circulante, supera el valor de reserva reportado por el oráculo, la transacción se restringe.

3.2.3 Segregación de activos digitales

En la fase inicial, mientras solo Wenia puede custodiar USDW, se utilizan billeteras separadas para distinguir el USDW propiedad de Wenia del USDW perteneciente a clientes. Con el tiempo podrían establecerse billeteras adicionales según las necesidades operativas.

El USDW de clientes se identifica dentro de una estructura de cuenta ómnibus para soportar una atribución correcta de saldos. Wenia también mantiene un marco de custodia que gobierna el almacenamiento y

protección de los criptoactivos bajo custodia, incluido USDW.

3.3 Funciones

El estándar ERC20 ofrece amplia compatibilidad y flexibilidad para el diseño del token.

3.3.1 Funciones ERC20

a) Mintage: la función mint permite controlar la creación y el suministro del token.

b) Transferencia: la funcionalidad de transferencia permite intercambiar USDW entre titulares mediante transacciones on-chain rápidas y seguras.

c) Balance: la función balanceOf permite consultar el saldo asociado a una clave pública determinada.

3.3.2 Extensiones ERC20

a) Quemable: la función burn permite controlar el suministro del token.

b) Seguridad: la funcionalidad pausable permite pausar y reanudar operaciones en caso de emergencia; la actualizabilidad permite mejoras y cambios de parámetros; y el control de acceso restringe funciones críticas a usuarios autorizados.

3.3.3 Parámetros de Wenia

a) Listas restrictivas (denylist): USDW incluye funcionalidad para restringir direcciones no autorizadas y, en circunstancias excepcionales, destruir

fondos mantenidos por direcciones restringidas luego de un incidente de seguridad, una investigación o un requerimiento de autoridad.

b) Umbrales: los umbrales de transferencia y de mint/burn ayudan a gestionar riesgos y apoyar controles de cumplimiento.

4. Seguridad

La seguridad es una prioridad para Wenia. El modelo operativo de USDW incorpora auditorías externas, monitoreo en tiempo real, controles de ejecución basados en MPC y arquitectura de contrato actualizable.

4.1 Auditoría

El marco de contrato inteligente de Wenia es auditado por OpenZeppelin, reconocido líder en seguridad Web3. La auditoría cubre la lógica del contrato, la resiliencia frente a vectores de ataque comunes y la alineación con mejores prácticas de desarrollo.

4.1.1 Explorador de bloques

Los exploradores de bloques brindan visibilidad sobre transacciones y contratos inteligentes, mejorando la transparencia y la revisión independiente.

a) Contrato inteligente verificado: un contrato verificado pone su código fuente a disposición pública y lo alinea con el bytecode desplegado.

b) Auditabilidad del código: la disponibilidad pública del código permite revisión por expertos independientes y por la comunidad.

4.2 Monitoreo

Wenia opera un sistema de monitoreo que supervisa interacciones con el contrato inteligente en tiempo real y genera alertas frente a actividades sospechosas como superación de umbrales, patrones anómalos o intentos de acceso no autorizados.

4.3 MPC

La Computación Multipartita (MPC) se utiliza para despliegues, actualizaciones y ciertas acciones críticas del contrato inteligente como alternativa segura a enfoques tradicionales de multifirma.

4.3.1 Políticas de ejecución del contrato inteligente

Las políticas de ejecución basadas en MPC incluyen iniciación de propuestas por operadores autorizados, periodos de revisión predefinidos y controles de acceso que limitan la aprobación y ejecución a partes autenticadas con los permisos requeridos.

4.4 Actualizaciones del contrato

La actualizabilidad del contrato permite a Wenia mejorar funcionalidad, remediar vulnerabilidades y adaptarse a requerimientos regulatorios u operativos. USDW utiliza el estándar UUPS (Universal Upgradeable Proxy Standard).

4.4.1 Proxy UUPS

UUPS incorpora la lógica de actualización dentro del contrato de implementación, reduciendo superficies de ataque y mejorando la eficiencia.

4.4.2 Implementación UUPS en USDW (Proof of Reserve)

Dirección del proxy en Ethereum:

<https://etherscan.io/token/0x131522cad80c0c45c014eb484af41df5af311721>.

Dirección de la implementación en Ethereum:

<https://etherscan.io/address/0xb467c1d3d1a751571c2c8f9cc34011b07d4e4890>.

4.5 Segregación de funciones y responsabilidades

Wenia separa responsabilidades del contrato inteligente entre roles de seguridad, gestión financiera, cumplimiento y administración.

Estos roles incluyen permisos para grant/revoke, actualizaciones y pausas de seguridad, funciones mint/burn, gestión de parámetros financieros, controles de cumplimiento y funciones administrativas de respaldo.

5. Regulación de USDW

USDW es emitido por Wenia Ltd., sociedad incorporada en Bermudas y licenciada con una licencia Clase F para desarrollar

negocios de activos digitales conforme a la Digital Asset Business Act 2018. Su emisión y operación, por tanto, están sujetas a los estándares prudenciales establecidos por la Autoridad Monetaria de Bermudas.

5.1 Ambiente de operación regulado

Wenia opera bajo requerimientos que incluyen normas de gobierno corporativo, cumplimiento AML/KYC/KYT, gestión de riesgo operativo, seguridad de la información y ciberseguridad, gestión de riesgo financiero y exigencias de transparencia y seguridad aplicables a las reservas.

5.2 Derechos de los titulares de USDW y obligaciones de Wenia

Los titulares de USDW no tienen título legal sobre las reservas creadas por Wenia mediante la estructura fiduciaria segregada. Sus derechos recaen sobre USDW como activo digital y no sobre moneda fiat ni sobre los activos de reserva.

Los titulares de USDW no tienen derecho a recibir intereses o valorización sobre sus tokens, incluso si Wenia obtiene rendimientos sobre los activos de reserva. En principio, los titulares pueden circular USDW entre usuarios de Wenia y convertirlo a otros activos digitales disponibles en la plataforma. Wenia también trabaja para ampliar la interoperabilidad con billeteras externas.

Los terceros titulares de USDW pueden redimir el token a través de Wenia al precio de referencia indicado en el contrato inteligente, sujeto a los términos aplicables y a las políticas operativas. En caso de insolvencia, liquidación o imposibilidad de continuar operando, la estructura de reserva está diseñada para apoyar esfuerzos de recompra manteniendo el objetivo de referencia 1:1.

Los derechos y obligaciones de Wenia y de los titulares de USDW se rigen por los Términos y Condiciones publicados en www.wenia.com y por las divulgaciones de riesgo publicadas en el sitio web de Wenia.

6. Referencias

1. Banco Agrícola S.A., Corporate and Financial Services Information. Banco Agrícola, El Salvador. Available online: <https://www.bancoagricola.com/>

2. Arévalo Segovia y Asociados, S.A. de C.V., Professional Audit, Accounting, and Advisory Services. Official firm website, San Salvador, El Salvador. Available online: <https://ars-asociados.com/>

3. Chainlink Labs, Chainlink Documentation – Proof of Reserve Data Feeds. Chainlink Documentation, 2026. Available online: <https://docs.chain.link/data-feeds/smartdata#proof-of-reserve-feeds>

4. F. Vogelsteller and V. Buterin, EIP-20: ERC-20 Token Standard. Ethereum Improvement Proposals, 2015. Available online: <https://eips.ethereum.org/EIPS/eip-20>

5. OpenZeppelin, OpenZeppelin Contracts Documentation. OpenZeppelin, 2026.

Available online:

<https://docs.openzeppelin.com/>